5.7 NUCLEAR CRITICALITY SAFETY ANALYSIS (NCSA) GUIDELINES. This section provides general discussions and guidelines for analyzing and establishing controls for ensuring nuclear criticality safety (NCS) at DOE nonreactor nuclear facilities and fuel handling/storage areas within reactor facilities where the potential for a criticality accident exists by virtue of handling, processing, or storing fissionable materials. It is applicable to the performance of nuclear criticality safety analyses for new facilities and modifications to existing facilities that may influence the nuclear criticality safety of significant quantities of fissionable materials. A "Graded Approach" should be used as described in section 5.6.4.

5.7.1 Scope. The scope of this section is limited to analysis guidelines associated with nuclear criticality safety and does not include other elements of the nuclear criticality safety analysis process, such as the nuclear criticality safety evaluation, nor requirements for control of the engineering design process. For this guide, nuclear criticality safety is the effort to prevent an unplanned and uncontrolled nuclear fission chain reaction. Unlike typical facility industrial safety, nuclear criticality safety is not based on a wealth of historical accident data. It is dependent on the best judgment of personnel assigned to design, analyze, operate, and monitor facilities and operations involving fissile and fissible (fissionable) material.

5.7.2 Identifying the Need for a NCSA. Operating organizations are responsible for identifying the need for a new or revised NCSA. However, other organizations, such as the criticality safety organization, may bring the need for a new or revised NCSA to the attention of an operating organization. In keeping with the requirements of section 2.1.10, a new NCSA is required before a new fissionable material handling, processing, or storage operation is implemented. A new, or revised, NCSA is required whenever an existing operation involving the handling, processing, or storage of fissionable material is changed beyond the scope of existing NCSAs and established limits. Changes that may require a new or modified NCSA include, but are not limited to, changes or modifications in

- the location of a piece of equipment or glovebox in which fissionable material will be handled, processed, or stored;
- the geometry of a piece of equipment that will contain fissionable material or a change in the geometry of fissionable material itself;
- fissionable material nuclide or enrichment;
- physical or chemical form of the fissionable material;
- the density or concentration of the fissionable material;
- the quantity of fissionable material or batch size;
- the moderation or reflection of fissionable material;
- a processing sequence involving fissionable material;
- the method of containment of fissionable material;

- the method or location of storing fissionable material, including changes in the spacing of containers or type of containers;
- the quantity or type of neutron poisons, including changes in the decision to use or discontinue use of neutron poisons;
- the method of moving fissionable material within a facility or around the site;
- credible errors or accidents, or change in the probability of accidents, in handling, processing, or storing fissionable material; and
- passive or active engineered controls or administrative controls whose purpose is to satisfy the double-contingency principle, including changes in the type of equipment, its independency, or its reliability.

5.7.3 Overview of the Nuclear Criticality Safety Analysis Process. Nuclear criticality safety is achieved through design and administrative measures. A criticality accident is prevented by controlling various nuclear parameters that influence the potential for criticality. These nuclear parameters include: (1) mass of material, (2) concentration of material, (3) geometry of material and equipment containing material, (4) degree of moderation and reflection, (5) spacing of, and interaction among, units containing fissionable material, (6) enrichment of the fissionable isotopes, and (7) the degree of neutron absorbers (poisons).

5.7.3.1 Major projects. At the beginning of facility design or modification, facility, equipment, and process criteria (design criteria) are established, and major systems are identified. As the design evolves, processes and equipment are identified, flow rates and production rates are established, and the types, volumes, and masses of fissionable material and associated materials are identified. The number and locations of connections of process lines and needed auxiliary systems, equipment, and materials are also incorporated into the design. Throughout the design process, there are various types of reviews that shall be conducted. The following important reviews ensure that nuclear criticality safety is properly incorporated into the design.

5.7.3.1.1 Preliminary process hazards review. Prior to the issuance of a Functional Design Criteria, a Preliminary Process Hazards Review should be performed to determine if the facility will be handling fissionable materials, regardless of amounts or concentrations, and whether the potential exists for a nuclear criticality accident. If it does, the Preliminary Process Hazards Review Report should state as an action item that the design should comply with the general principles and objectives presented in this document, including application of the double-contingency principle (see section 5.7.8).

5.7.3.1.2 Design process and design reviews. It is imperative that design considerations affecting nuclear criticality safety begin very early in the design process. Information will be required from a nuclear criticality specialist that provides quantitative data on the limits for various parameters that influence criticality that, if exceeded, could result in a criticality accident. These data will depend on the types and forms of the fissionable materials involved. As is common to any design process, an iterative approach is required to arrive at a design concept that is both acceptable and optimized from a nuclear criticality safety standpoint. An illustration of the general iterative process for implementing nuclear criticality safety is shown in Figure 5.7.3.1.2-1. The goal for the final design should be the attainment of the six basic design objectives presented in section 5.7.4. The Design

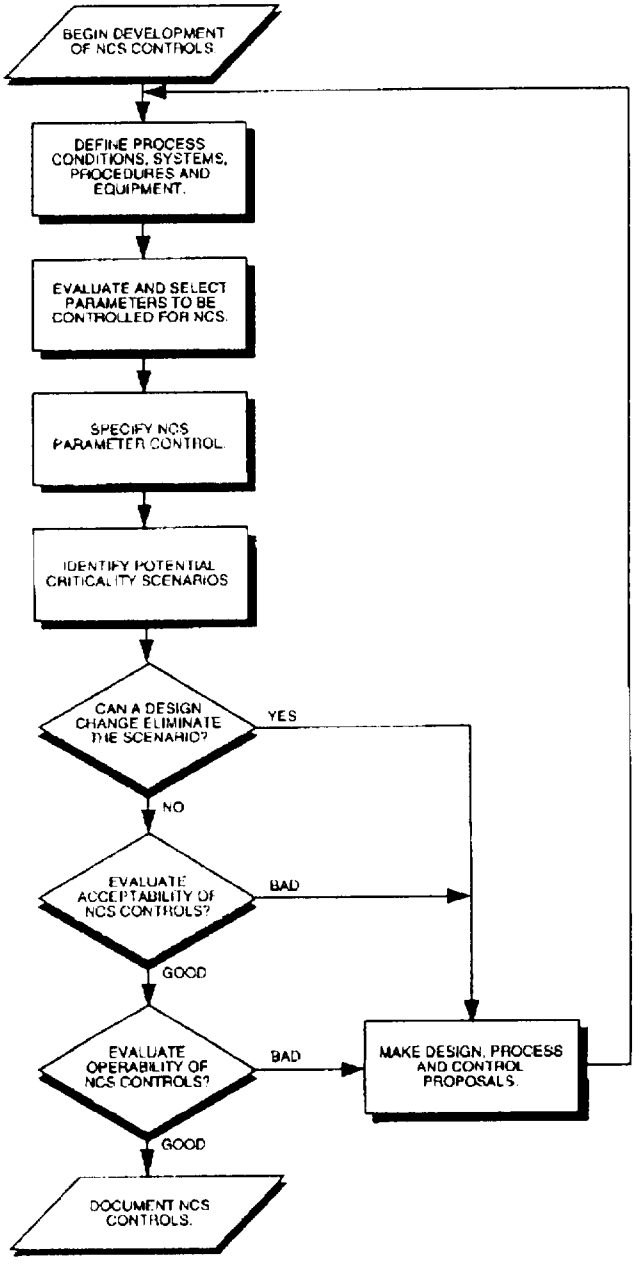

Figure 5.7.3.1.2-1. Illustration of iterative process for development of nuclear criticality safety controls.

Process Hazards Review (conducted by the design organization, operations personnel, and a cognizant nuclear criticality safety specialist) should confirm design adequacy relative to the six basic objectives, including documentation of the application of the double-contingency principle.

5.7.3.1.3 Preoperational process hazards review. The design process (section 5.7.3.1.2) shall identify criticality hazards associated with the design concept and provide appropriate controls. However, the Preoperational Process Hazards Review (that is conducted by facility management with assistance from the cognizant nuclear criticality safety specialists) offers an excellent opportunity to independently review design adequacy relative to nuclear criticality safety and to implement improvements prior to start-up, as needed. Documentation of the design, as specified in section 5.7.10, should provide a major information source for this review. The preoperational review should

(a) confirm design adequacy as measured against the six basic design objectives presented herein (paragraph 5.7.4),

(b) confirm that facility, equipment, and process conditions conform to the intended design,

(c) examine the nuclear criticality safety control methods and the means of control incorporated in the design, and confirm the judgments made during the design process as to the expected reliability of such controls,

(d) review the results of Deductive Logic Tree Analyses, Inductive Logic Tree Analyses, Failure Modes and Effects Analyses, Direct Accident Postulation, or others performed on the design (if available) for any insights into potential areas of weakness,

(e) identify, based on the above, any design improvements relative to nuclear criticality safety, as needed, and

(f) ensure that all nuclear criticality safety controls, either implemented by initial design or by follow-up improvements, are properly documented, such as by analyses, procedures, and drawings. In this regard, it is important to maintain a documented trail of the application of the double-contingency principle.

The preoperational review should cover the conduct of facility operations to include configuration control and maintenance policies that will govern the operation, care, and preservation of those engineered and administrative controls that are of importance to nuclear criticality safety.

5.7.3.2 Projects involving modifications to existing equipment.

5.7.3.2.1 Screening process hazards review. Cognizant nuclear criticality safety specialists should identify hardware for which proposed changes must receive nuclear criticality safety analysis prior to implementation. Care should be taken to ensure that the double-contingency principle is not compromised. Documentation of double-contingency considerations should be maintained. Modifications that involve a loss or compromise of nuclear criticality safety controls, particularly loss of double-contingency, should be reviewed as potential unreviewed safety questions (USQs).

5.7.3.2.2 Preliminary process hazards review. If the screening process hazards review requires resolutions of issues among several technical disciplines, a preliminary process hazards review team may be formed for the purpose of resolving these issues.

5.7.3.2.3 Preoperational process hazards review. Action items are reviewed as described in section 5.7.3.1.3 during the Preoperational Process Hazards Review. Issuance of the final Preoperational Process Hazards Review indicates closure of all action items, proper documentation of all action items (including double-contingency), and formal acceptance of the action items as described by responsible line management.

5.7.4 Six Basic Nuclear Criticality Safety Analysis Objectives. Risk control for nuclear criticality safety is primarily directed toward reduction of accident probability by means of process controls. In arriving at a final nuclear criticality safety analyzed and approved equipment/process concept, focus should be directed toward achieving six basic nuclear criticality safety analysis objectives discussed in this section.

5.7.4.1 Objective 1 - to control criticality probability using a preferred hierarchy of controls. A variety of criticality safety control methods exist that may be considered for application in a given case, such as geometry control, spacing control, and mass control. Not all methods of control are equally preferred. Three basic means of control (passive-engineered, active-engineered, and administrative) are presented and ranked in order of preference, and are discussed later in section 5.7.5, "Means of Controlling the Criticality Risks," where this objective is discussed in detail.

5.7.4.2 Objective 2 - to identify potential criticality scenarios. A necessary step in evaluating and controlling a risk is recognizing its existence. Even though many potential paths to a criticality event will be obvious, other potential paths will not be obvious. Section 5.7.6, "Identifying Potential Criticality Scenarios," expands upon this objective. Four important approaches to successful identification are discussed. A deductive logic tree approach is illustrated with an example.

5.7.4.3 Objective 3 - to eliminate potential criticality scenarios to the extent practical. Although a potential criticality scenario may be shown to meet the minimum standard for acceptability (Objective 4), it is preferred, whenever feasible, that the risk be eliminated entirely from the fissionable material process, even though the probability of occurrence of a given criticality accident scenario is less than some minimum acceptable level. It is better to modify the equipment or process, if possible, to eliminate the scenario entirely. A review of the equipment or process concept should be performed searching for feasible changes that will eliminate a potential criticality scenario. Elimination can be achieved by facility, equipment, or process changes that act to remove the initiating event from an accident sequence. For example, a change from water cooling to air cooling in a given process may eliminate a scenario involving the potential for undesirable moderation. This objective is discussed in section 5.7.7, "Eliminating Potential Criticality Scenarios."

5.7.4.4 Objective 4 - to demonstrate that criticality risks are unlikely. Protection against a criticality accident should involve a defense-in-depth approach in which multiple, independent, unlikely events must occur before a criticality accident is possible. Section 5.7.8, "Judging Acceptability of a Potential Criticality Scenario," where this objective is discussed further, provides a means to judge acceptability based on the double-contingency principle. In the completely analyzed facility, the equipment and process concept should have each potential criticality scenario identified and should meet the minimum standard for acceptability presented in this section.

5.7.4.5 Objective 5 - to evaluate the operability of criticality safety controls. Selections made during the facility equipment and process design or modification will have a significant effect on the degree of difficulty presented to facility personnel in operating the facility. Section 5.7.9,

"Operability of Criticality Safety Controls," discusses this objective and presents nine specific considerations for facility operations.

5.7.4.6 Objective 6 - to document the nuclear criticality safety analysis and controls. Proper documentation of all facility, equipment, and process aspects important to nuclear criticality safety is essential for use by personnel in the areas of nuclear criticality safety analysis, facility operation, engineering design, design review, and auditing. The elements of proper documentation are presented in section 5.7.10, where this objective is discussed further.

5.7.5 Means of Controlling the Criticality Risks.

Objective 1 - criticality risks are controlled using a preferred hierarchy of controls. Nuclear criticality safety is achieved by exercising control over various nuclear parameters. Section 5.6.3 describes nuclear parameters that may be controlled for nuclear criticality safety, however, the means of control addresses how the control is achieved in design and operating terms. These nuclear parameters consist of the physical form, mass, and distribution of fissionable materials, and the physical form, mass, and distribution of all other materials with which the fissionable materials are associated. Eight such criticality control methods, each associated with the nuclear parameter controlled for nuclear criticality safety, are (1) geometry control, (2) spacing control, (3) neutron poisons control (fixed and soluble), (4) concentration control, (5) moderation and reflection control, (6) mass control, (7) enrichment control, and (8) density control. A subtle combination of these nuclear parameters is the inherent form of a material that may require "form control" to prevent conversion of the material form from, say, UF_6 to UO_2F_2, or from UF_6 and HF gas to a liquid. Additionally, spent nuclear fuel exhibits inherent combinations of controls 1 through 8, in their respective passive forms, in that it has specific physical constraints on geometry, or rod or pin spacing, resulting in limiting degree of moderation, neutron absorbing fission product inventory, and depleted fissionable material enrichment, mass, and concentration. A given situation may call for employing more than one of these control methods.

The "control method" refers to the nuclear parameter being controlled. The "means of control" refers to the design/operating mechanism achieving the control. The three basic means of control are (1) passive-engineered control, (2) active-engineered control, and (3) administrative control. For example, concentration control may be achieved by means of an active engineered control such as an eductor (an automatic dilution device) and by means of an administrative control such as sampling. These means of control are not equally preferred for nuclear criticality safety. The passive-engineered means of control is most preferred, followed by active-engineered control, and then administrative control. Guidance in the preferred use of the basic means of control is provided in section 5.7.5.1.

A discussion on the use of each of the eight control methods is provided in section 5.7.5.2, including the definition and use; the typically associated means of control; the reliability, range of coverage, and operational support required; and the common failure modes. Control methods that typically employ the more highly preferred means of control should be selected, whenever practicable. For example, geometry control is generally implemented using passive-engineered design features, which is a highly preferred means of control. In contrast, concentration control is generally implemented using active-engineered and administrative controls, which are less preferred. Table 5.7.5-1 shows the nine control methods ("eight" has become "nine," distinction being made here between moderation and reflection) and the typically associated means of control.

Table 5.7.5-1. Criticality Safety Control Methods and Typically Associated Means of Control

CONTROL METHOD	ASSOCIATED CONTROL MEANS (TYPICAL)		
	PASSIVE ENGINEERED	ACTIVE ENGINEERED	ADMINISTRATIVE
GEOMETRY CONTROL	X		
SPACING CONTROL	X(FIXED)	X(MACHINE AUTOMATED)	X(PROCEDURAL)
NEUTRON POISON CONTROL	X(FIXED)	X(SOLUBLE)	X(SOLUBLE)
FISSIONABLE MATERIAL CONCENTRATION CONTROL		X	X
FISSIONABLE MATERIAL DENSITY CONTROL		X	X
MODERATION CONTROL	X(FIXED)	X	X
REFLECTION CONTROL	X(FIXED)	X	X
ENRICHMENT CONTROL		X	X
FISSIONABLE MATERIAL MASS CONTROL			X

5.7.5.1 Three basic means of criticality safety control. As discussed above, the three means of managing the nine criticality safety control methods are passive-engineered control, active-engineered control, and administrative control. The ranking of the three means of criticality safety control is intended as a general guide of preference. In practice, a case-by-case evaluation is required to determine the best control method and means of control available for each circumstance, considering the unique requirements and conditions in existence at the time. All control methods generally have some degree of administrative dependence or other features that make it difficult to categorically assign a means of control to a particular control method.

5.7.5.1.1 Passive-engineered control. Passive-engineered control is the highest ranked means of criticality safety control, involving fixed, passive design features or devices rather than moving parts. These means of control are highly preferred because they provide high reliability, a broad range covering many potential criticality accident scenarios, and require little operational support to maintain effectiveness. Human intervention is not required. Advantage is taken of natural forces, such as gravity, rather than electrical, mechanical, or hydraulic action.

5.7.5.1.2 Active-engineered control. Active-engineered control is a means of criticality safety control, of intermediate rank, involving add-on, active electrical, mechanical, or hydraulic hardware that protects against criticality. These devices act by sensing a process variable important to nuclear criticality safety and providing automatic action to secure the system in a safe condition without human intervention. Active-engineered controls are preferred when passive-engineered controls are not feasible. These devices are subject to random failure and to human error occurring during operations and maintenance activities. Therefore, high-quality, low-failure-rate equipment should be selected in all cases. Fail-safe designs should be employed, if possible, and failures should be easily and quickly detectable. The use of redundant systems should be considered as a means of dealing with unavailability. Active-engineered devices require surveillance, periodic functional checks, and preventive and corrective maintenance to maintain effectiveness.

5.7.5.1.3 Administrative control. Administrative Control is a means of criticality safety control that relies on the judgment, training, and responsibility of people for implementation. These controls may be action steps or caution steps in an operating procedure or steps in a surveillance program. Because they are human-based, and subject to error in application, administrative controls are generally regarded as the least desirable means of criticality safety control. In some instances, however, reliance must be placed on this means of control. Where practical, processes, equipment, and necessary instrumentation should be designed to initiate and facilitate human intervention or discourage misoperation. An example includes the design of handling or process equipment that limits the number of units or mass of fissionable material that a fissionable material handler can transfer. Where practical, administrative controls should be augmented by warning devices (visible or audible) that mandate operator action according to a specified procedure. Activation of warning devices should be minimized in order to be effective.

5.7.5.2 Criticality safety control methods. The following subsections list control methods used for nuclear criticality safety and discuss passive-engineered control, active-engineered control, and administrative control, and considerations associated with each.

5.7.5.2.1 Geometry control. Geometry control is the preferred method of criticality safety control based on limiting one or more characteristic dimensions. Where practicable, reliance should be placed on the use of geometry control rather than the control of any other nuclear parameter. The practicality of using geometry control depends on the type of equipment needed (it may be impossible to incorporate a geometrically safe design for a large-scale pit), the process flow rates and volumes, and inherent complexity. Because each system and facility may be different, decisions shall be made and approved on a case-by-case basis.

Geometry control is based on physical design limits, such as "geometrically safe" or "geometrically favorable" cylinder diameter, annulus inner and outer diameter, slab thickness, and spherical diameter (and the closely related concepts of "safe" or "favorable" volume) for a given fissionable material. Geometrically safe is defined as the characteristic dimension of importance for a single unit of a specific geometrical shape such that nuclear criticality safety is not dependent upon any other nuclear parameter. A geometrically safe dimension is determined assuming optimal moderation, thick reflection, and no control on concentration, enrichment, mass, or neutron poison. Geometrically favorable is defined as the characteristic dimension of importance for a single unit of a specific geometrical shape such that nuclear criticality safety is maintained in conjunction with one or more other nuclear parameters such as concentration and limited reflection.

If geometrically favorable dimensions are used, care shall be taken to guard against the possibility of losing control over the other nuclear parameters upon which favorable geometry depends. Geometrically favorable control may require active protective devices or administrative controls, or both, such as concentration- or moderation-control monitoring equipment, on-line enrichment- or mass-control monitors, and sampling. If there is no possibility that the geometrically favorable conditions will be violated (for example, the facility only handles uranium having 10% enrichment or less, or there is no credible way for the material to become reflected or moderated), then it may be reasonable to consider the geometrically favorable dimensional parameters as passive-engineered control rather than as active-engineered or administrative control.

Geometry control limits (if maintained) preclude the possibility of criticality by virtue of neutron leakage from the system. This control method provides inherent criticality protection that (1) is not subject to random failures (as may occur with an "active" control device), (2) is not susceptible to the common types of human errors occurring during operating and maintenance activities that may act to defeat the control, and (3) provides inherent protection against unforeseen criticality scenarios. This control method requires a minimum of facility operational support to maintain effectiveness. Note that spacing between geometrically safe units shall be considered because of the potential for interaction.

Geometry control has many applications. Arrays of geometrically controlled cylindrical columns or slab tanks may be used to store or process fissionable material solutions. Geometrically controlled slab geometry may also be used for drip pans and for tables used for cleaning small pieces of contaminated equipment with various solutions. Process piping and drain lines often need to be designed to be geometrically controlled. Other equipment or portions thereof that normally do not process or contain fissionable material may also need to be controlled by volume or geometry. For example, if significant quantities of fissionable material can enter lubricating oil in a pump, the pump and its oil reservoir, if any, may need to be limited in size to a safe volume. Alternatively, it may be necessary to conservatively approximate the geometry of the interior of the pump and any oil reservoir and perform calculations to show that the geometry is safe for all credible cases.

5.7.5.2.1.1 Geometry control applied to process and storage vessels, equipment, and containers. As discussed above, geometrically controlled cylinders, slabs, annuli, and spheres may be used for process and storage vessels. Loss of safety could result from various phenomena, such as abnormally high pressure, causing dimensional distortions to the point that the critical dimension is reached. Even though a spherical geometry is the shape of choice from the standpoint of dimensional stability, a spherical tank often has limited practical use because of restrictions on useful volume. Elongated cylindrical geometries have favorable characteristics under pressure and have been used successfully for a wide range of applications. Annular and slab geometries are subject to distortions under pressure; however, in many applications these shapes can be adequately stabilized using external bracing and internal stay-bolts or tie-rods.

Even though a vessel may be designed to be geometrically safe or favorable, solution absorbing insulation or liquid heat exchanger jackets that surround the vessel may invalidate geometry control. If absorbing insulation or liquid heat exchanger jackets are required to be placed around a geometrically controlled vessel, precautions should be employed to ensure that vessel leaks will not accumulate unsafely in the insulation or heat exchanger jacket. A common practice in the use of liquid heat exchanger jackets is to maintain the pressure of the fluid in the heat exchanger jacket higher than the pressure inside the vessel. A differential pressure monitor and corresponding alarm may be necessary.

Corrosion of the vessel walls should also be considered. Over time, corrosive attack causing a uniform thinning of the vessel wall will increase the inside dimension to a value greater than the as-built value at the beginning of service life thereby reducing original margins of subcriticality. In addition, corrosion of the vessel walls and structural members may cause structural weakness, and thus increase the potential for bulging or rupture under pressure. If necessary, a "weep hole" concept should be considered as a means of detecting excessive corrosion. This can be accomplished by drilling several holes from the outside of the tank to about 0.5 wall thickness. For vessels using geometry control, corrosion leading to the loss of contents by leaks is not a criticality problem in itself, if suitable provisions are made in the design for dealing with the leaking solution. Therefore, an allowance for corrosion shall be included in the design of a vessel in which corrosion may occur.

Because dimensions are of great importance for the maintenance of geometry control, designers and criticality specialists must understand each other when it comes to designing and implementing dimensions calculated for nuclear criticality safety. For example, to a criticality specialist, it is easy to perform a calculation using exact dimensions for a 5.000-in. pipe I.D. However, when translated to actual design, it may be difficult, or impossible, for a designer to order material of the exact dimension used by the criticality specialist in his/her calculation. It is important, then, that the criticality specialist understand that a designer may be limited to a certain material. It is equally important that a designer understand that an exact dimension may be crucial to nuclear criticality safety. If commonly available materials differ dimensionally from those used in nuclear criticality safety calculations, then the material selected should be less than the geometrically controlled dimension of importance, or additional calculations shall be performed using dimensions of the various materials that are available (in which case, additional controls may be needed if the geometrically controlled dimension cannot be maintained).

When multiple units or arrays of geometrically controlled equipment are needed, proper spacing and the buildup of fissionable material between units shall be considered. Even though an individual unit may be geometrically controlled, safe spacing of the equipment units shall be calculated to limit neutron interaction, or the equipment units shall be neutronically isolated (decoupled) from each other by the use of thick reflection or neutron poisons, or both, around/between each piece of equipment. The buildup of fissionable material from overflows or leaks between adjacent units should be minimized because it defeats the geometrically controlled condition. Buildup can be a significant problem in slab tank arrays where it is crucial to maintain space between tanks free of accumulations and where it is difficult to inspect and clean such locations. Care shall also be taken to consider the neutron interaction due to intersections of connecting piping and drains with geometrically controlled equipment.

Frequently, processes cause a transformation of fissionable material characteristics, such as in the high-temperature melting of low-density feed materials to high-density metals or alloys, or the chemical conversion of compounds to metals or metals to compounds. In any instance, consideration shall be given to intermediate conditions of the material throughout the transformation.

In the instance of casting reduced-density, yet compacted, metal machine turnings into solid metal ingots, consideration should be given to the following:

(a) providing a safely subcritical environment for a large volume of compacted machine turnings within a casting crucible,

(b) providing a smaller limited volume/shape molten casting charge,

(c) providing a safely subcritical environment for a casting mold of solid frozen metal,

(d) providing catch basins, rings, or other devices for casting mishaps such as broken crucibles, leaking pour diverters, and broken or leaking molds, and

(e) replacing worn and potentially oversized molds.

Overflow holes in crucibles and molds play an important role in limiting the molten mass of metal within crucibles. Likewise, overflow holes in molds prevent incomplete crucible discharges to a mold or undesirable casting configurations.

The wearing of extrusion press dies and wire drawing dies generally affects product or process quality prior to affecting nuclear criticality safety. However, such equipment wearing or aging should be considered because it may affect the nuclear criticality safety of the product material by permitting the pressing or drawing of oversized materials.

5.7.5.2.1.2 Geometry control applied to facility features (e.g., placement and depth of curbs, sumps, stairwells, elevator shafts, door sills). Provisions shall be made in facility design to consider leaks of significant quantities of fissionable material from process and storage vessels, equipment, containers, interconnecting piping, and instrumentation ports and tubing. Solutions containing fissionable material shall not be allowed to accumulate in an unsafe geometry. Thus, geometry control is often used in connection with sump design. Typically, a sump is designed with a flat bottom so that liquid initially accumulating in the sump takes on the shape of a geometrically safe or favorably thin slab. When applying this concept, protection shall be provided so that the maximum credible liquid level (considering the fissionable material of interest at optimum moderation) in the sump at any time will be less than the minimum critical slab thickness obtained from calculations or appropriate tables. One means of providing this protection on maximum liquid level is to incorporate an overflow capability so that excess liquid present in the sump will overflow to a safe region. Protection shall be provided against loss of overflow capability. The design should be such that no single object present in the sump can block the overflow, such as a rag or other object, nor should accumulations easily plug it. The maximum credible volumetric liquid flow rate to the sump shall not exceed the design dump-out rate. Protection shall be provided against unwanted seepage into the sump and corrosion of the sump material. With prolonged exposure to reactive chemicals, like evaporating acids, it is possible for solutions of fissionable material to seep into and under sumps unless they are adequately lined. The possible "sloshing" of a sump's contents during filling should be considered because of induced wave motion that may exceed safe or subcritical liquid thicknesses.

If conditions do not permit overflow capability, it is important to ensure that the liquid level in the sump corresponding to the maximum credible addition of solution (from a worst-case leak or vessel rupture of fissionable material) will be less than the minimum critical slab thickness. If the liquid level cannot be controlled because of potential large additions of liquids containing fissionable material, then the use of solid neutron poisons such as Raschig rings should be considered (see section 5.7.5.2.3.1).

5.7.5.2.1.3 Minimizing holdup volume and geometry in auxiliary process equipment. Geometry control is a very effective means of providing inherent criticality protection for equipment items not

intended for fissionable material processing or storage (such as pumps, valves, and filters). This control may be achieved by limiting the maximum holdup volume in an equipment item to less than the minimum critical volume for the fissionable material being processed, as determined by calculations or applicable tables.

Additionally, in areas having overhead liquid fissionable material process lines or storage vessels, policies and procedures shall be established to deter incidental or unintentional containers such as unrestricted volume tool boxes, mop buckets, sponges, mops, open-topped plastic-lined containers, or other containers that could collect liquids.

5.7.5.2.1.4 *Passive devices preventing geometrical distortion, improper orientation, or solution* transport. This group ranks high in the preference sequence. Because of simplicity and the absence of moving parts, the reliability of items in this group is high, while operational support requirements are generally low. Often, items in this group compete with, but are preferred to, the use of active protective devices to provide similar safety functions.

Potential criticality problems may be caused by the distortion of a geometrically safe shape or the unwanted and unexpected transport of liquids from safe to unsafe locations. Fixed, passive design features and devices are available to prevent such occurrences. Examples of these devices and design features include rupture disks, vents (with overflow to a geometrically safe or favorable location), air breaks, barometric seal legs, nuclear safety blanks, large (but safe) line sizes, restricting orifices, and relative elevations. *Section D.3 contains additional information on each of these* devices and techniques. Of particular interest are air breaks and barometric seal legs. These two items provide effective protection and should be incorporated as standard practice, as applicable.

5.7.5.2.2 Spacing control. Spacing is a highly preferred method of control consisting of the use of passive devices or systems, or administrative controls, to ensure the maintenance of favorable spacing. Safe spacing maintains neutron leakage and reduces neutron interaction among units containing fissionable material.

Fixed (passive) spacing controls are used for the separation of fissionable material in operating activities and storage of many types of fissionable materials including weapons components, wet or dry *storage of reactor fuel, storage of oxides or nitrates,* storage of fissionable material in shipping containers, and storage of fissile-containing solutions. Examples of such devices and systems include pool storage racks, floor storage racks of various types, dollies having a base of sufficient dimensions to provide favorable spacing, fissionable material birdcages, and safely spaced shelving. To be considered a strictly passive control, spacing shall not be dependent on other nuclear parameters, or the other nuclear parameters shall be fixed. For example, spacing that also incorporates fixed neutron poisons is considered passively favorable spacing; spacing that passively limits container size to those containers that may be safely spaced is considered favorable spacing; spacing that is designed for materials having a limited enrichment is considered passively favorable spacing as long as other materials having higher enrichments are either not available or cannot fit into the safely spaced positions; and spacing that is designed for containers having limited moderation is considered passively favorable as long as containers without such moderation control limits are not available or cannot fit into the safely spaced positions. In situations where spacing is established for a specific container and its contents based upon specific mass, dimension, chemical composition, or fissile nuclide, features should be incorporated into the design to preclude the placement of other containers into the storage spaces. In addition, design features should eliminate the possibility of placing more than one container into a given storage space or placing additional

containers into the regions between storage positions. When the containers of fissionable material are relatively light and have low radiation levels such that they can be handled hands-on, the potential exists for human error, particularly in moving containers into and out of storage. It is better to design spaced arrays such that they cannot be easily defeated by human error rather than to rely strictly upon procedures. When several types of containers of fissionable material are to be stored in the same spacing structure, the spacing shall be established for the most reactive feasible combination of packages. This is normally the entire array filled with the most reactive package (although sometimes combinations of containers could be more reactive), and one position near the center double-batched if this is a possible loss of one control.

Passive control of spacing is highly reliable, not subject to random failures, and provides coverage against potential unforeseen accident scenarios. However, several problems with spacing are possible. Fixed (passive) spacing structures and devices may be susceptible to structural failures due to such conditions as exceeding the load limits, corrosion, ramming by forklifts, items falling from overhead cranes, and earthquakes. Spacing control may require the use of nondestructive gamma or neutron counting equipment or physical sampling and analysis to determine fissionable material package content before assigning a given spacing to a given package. In such situations, passive-engineered spacing control takes on aspects of active-engineered or administrative control. If a favorable spacing arrangement can potentially be defeated by human error or equipment failure, then it may be necessary to consider the spacing control as active-engineered or administrative in nature. In fact, it is sometimes difficult to strictly distinguish between passive spacing control and active-engineered or administrative spacing control.

If spacing control is dependent upon such things as signs, marks on the floor, procedures such as the spacing of packages 1 meter apart, or temporarily erected structures such as chained-off areas rather than fixed engineered storage structures, then it becomes administrative in nature and is less preferred than truly passive-engineered spacing design.

5.7.5.2.3 Neutron poisons. Neutron poisons preclude criticality by virtue of eliminating neutrons from a system through absorption. Absorbers may be fixed (solid) or soluble (in solution). Generally, fixed absorbers are considered passive-engineered controls, and soluble absorbers are considered active-engineered or administrative controls. Where practicable, vessel design should incorporate favorable geometry as a means of control before placing reliance upon neutron poisons. The practicality of using favorable geometry versus neutron poisons for solution processing is dependent upon the flow rate and volume of the solutions to be processed, the number of geometrically favorable units and parallel processing lines that may be required, the reliability associated with each unit, and the potential benefit of using neutron poisons to maintain safety while simplifying operations and improving reliability. For some items, it may not be possible to use a geometrically favorable design, thus, neutron poisons may be the only available means of nuclear criticality safety control.

Neutron poison control is generally not used for control of fissible nuclides because (1) fissible nuclides only fission with intermediate or fast neutrons, (2) few materials are good absorbers of intermediate and fast neutrons, and (3) simpler and easier methods of control are generally available.

5.7.5.2.3.1 Fixed neutron poisons. The use of permanently fixed, neutron-absorbing materials (poisons), such as boron-containing materials (borosilicate-glass Raschig rings, boral, borated stainless steel, borated concrete, borated polyethylene), cadmium, chlorine (PVC rings), or other solid neutron absorbing materials is considered to be a passively engineered method of criticality safety

control. In specific applications this method can provide inherent, reliable protection and shares many of the same advantages as passive-engineered geometry control and passive-engineered spacing control. However, the successful application of this criticality safety control method can vary widely, depending on the potential for various phenomena that can cause loss or redistribution of the absorber material and on the ease with which periodic verification can be made to confirm the continued presence of the absorber. Applications involving contact (or potential contact) of the absorber material with process solutions can cause loss of the absorber by leaching, general dissolution, or other chemical reactions. In such cases, cladding the absorber material may provide effective protection against chemical attack. Loss of absorber material can also occur by fire and physical damage. In all cases periodic verification tests will be required to confirm the proper amounts and distribution of absorber material and integrity of cladding. In some cases, such as remote applications of absorbers, verification testing may be quite difficult. Thus, it is important that provisions are made in the design to ensure that there is sufficient access to allow for periodic testing.

Raschig rings may be used to render otherwise geometrically unsafe vessels favorable depending on fissionable material concentration and packing density of the rings. Typical applications of Raschig rings include sumps, evaporator de-entrainment separator heads, large tanks, and scale pits. Packing density of the rings should not be overestimated when calculating the nuclear criticality safety of a vessel. Ring settling and boron leaching may also present problems. The detailed requirements for the use of borosilicate-glass Raschig rings are found in ANSI/ANS-8.5-1986.

Reactor fuel storage racks may be designed to incorporate various types of neutron poisons. Boral and borated stainless steel are typical neutron poisons that have been used in such storage racks. Borated concrete has been used for fresh fuel storage racks. Borated concrete is an example of a flux trap where the hydrogen content can vary as the concrete ages, therefore, the hydrogen content of borated concrete shall be verified or conservatively approximated.

Almost all materials absorb neutrons to some degree. Therefore, the "typical" materials of construction for a given facility may be important in maintaining the nuclear criticality safety of a given piece of equipment. If a nuclear criticality safety evaluation is made using a certain material, and another material is substituted in the design, nuclear criticality safety may be jeopardized. Whenever material substitutions are to be made, additional evaluations shall be performed to demonstrate that subcriticality and nuclear criticality safety are not compromised.

5.7.5.2.3.2 Soluble neutron poisons. Soluble absorbers are neutron-absorbing materials, such as boron in boric acid, gadolinium as gadolinium nitrate, or cadmium as cadmium nitrate, added to a solution for criticality safety control in vessels or piping that may otherwise be geometrically unsafe.

Control shall be exercised to maintain soluble neutron absorber continued presence with the intended distributions and concentrations. Extraordinary care should be taken with solutions of absorbers because of the difficulty of exercising such control. This method of criticality safety control is not preferred but has definite applications where the control methods discussed above are not applicable. The use of fixed neutron poisons should be investigated before placing reliance upon soluble absorbers. Neutron poisons, such as boric acid, are sometimes added to a dedicated water supply tank for fire fighting purposes in areas where unwanted moderation may be a concern.

Soluble neutron poisons are implemented using active-engineered and administrative controls. Administrative confirmation of the types and quantities of chemicals used for soluble absorber

makeup solutions is necessary, as well as a sampling of the prepared solutions themselves, to verify absorber concentration. Once prepared, solutions of soluble absorbers are sometimes subject to inadvertent precipitation of the absorber material from solution, the formation of distinct phases of the solution that have little or no absorber, or the dilution of the absorber by other makeup or process solutions. In many situations, soluble absorbers must be added for each use or batch requiring frequent operational support to ensure continued effectiveness.

Because of potential failure, it is best not to use soluble absorbers as a primary criticality safety control method. It is better to restrict the role of soluble absorbers as a secondary control method in the event that control of another nuclear parameter is lost such as exceeding fissionable material mass or concentration limits. Soluble neutron absorbers should not be used as the primary means of control if failure of the secondary control is not independent. For example, controls shall be established such that no single contingency may both increase concentration of fissionable species above the critical value (without poison) as well as cause poison to precipitate.

5.7.5.2.4 Fissile concentration control. Fissile concentration control is used in situations in which the concentration of fissile nuclides in solution must be controlled to maintain subcriticality in large (unfavorable geometry) tanks. At least two circumstances exist for which different emphases of concentration control are required. In the first circumstance, a physicochemical process of an operation may ensure that the fissile nuclide concentration of a solution will be within safely subcritical values. In such cases, the monitoring and control of concentration becomes a secondary control in the event the physicochemical process is corrupted or bypassed. In the second circumstance, processes involving potentially concentrated solutions of fissile nuclides can also use concentration control as one of the process variables to include as part of implementing double-contingency. Examples include large volumes of dilute waste solutions, such as raffinates from chemical extraction processes, evaporator condensates, or laboratory sample solutions that must be processed or stored in large and unfavorable geometry tanks or process equipment. However, as stated above, geometry control should be used, if practical.

Active-engineered or administrative means of control are normally used to implement concentration control. Procedures such as sampling, automatic concentration or density measurements with or without automatic shutoff valves, or prescribed dilution are always necessary since passive-engineered control of concentration generally is not feasible.

5.7.5.2.5 Moderation control. Moderating and reflecting materials (such as water, heavy water, acids, oil, plastic, beryllium, concrete, heavy metals, and carbon) tend to substantially reduce the quantity of fissile nuclides that may be safely handled. For this reason, processes involving fissile nuclide compounds or metals are often designed to specifically exclude or control the use of moderators. Moderation control is the purposeful control of the quantity of moderating material mixed with or intermingled with fissile nuclides. Fissile nuclides may be safely handled using moderation control in combination with other control methods, such as mass control and geometry control. In this way, larger masses of fissile nuclides in larger geometries may be handled than by using mass or geometry control alone. Measurement of the ratio of moderating atoms to fissile atoms may be necessary to verify moderation control (for example, in the case of aqueous moderation this ratio is expressed as the hydrogen-to-uranium or hydrogen-to-plutonium atom ratio). Because of the need to verify moderation level, moderation control is generally implemented using active-engineered and administrative controls such as sampling, drying, or moisture detectors. When implementing moderation control, designers shall take necessary steps to preclude potential sources of moderation (such as steam lines, water piping, tanks of aqueous solutions, beryllium powder,

hydrocarbons, and carbon materials) from areas handling fissile nuclide powders and solids. Doubly containing water pipes and employing a leak detection system between the inner and outer pipes is an acceptable compromise in many situations where water piping must pass through or over moderation controlled areas. Processes involving fissile nuclide powders and metals may also make use of suitable enclosures to reduce or eliminate the potential for unwanted moderation. Otherwise, a design should take suitable precautions for potential moderation and reflection and rely on other control methods.

Moderation control is an important consideration in selecting a fire control system. Available options include water, borated water, carbon dioxide, inert gases, and foam. See section 5.7.9.9 for more information.

When analyzing a fissionable material system consisting of fissible nuclides, it is important to understand the effect of added moderation to dry fissible nuclides. Since fissionable materials of fissible nuclides can only fission with intermediate or fast neutrons, the addition of moderators (that slow down neutrons to low energies) will make such materials less reactive to the extent that criticality may be precluded. On the other hand, when handling solutions of fissionable material constituted with fissible nuclides, consideration should be given to potential loss of moderation (due to evaporation or heating), which would make such systems more reactive.

Mixtures of fissible and fissile materials require special attention as they have conflicting contributions to the system reactivity depending upon the neutron energy spectra of the system.

5.7.5.2.6 Reflection control. Neutron reflecting materials (such as water, heavy water, concrete, steel, lead, plastic, beryllium, carbon, etc.) reduce the quantity of fissionable material that may be safely processed, stored, or transported. Generally, the degree of reflection evaluated for a given situation is taken to be the maximum credible available unless mitigating factors are, or reflection control is, ensured.

Reflection may be controlled to prevent unacceptable thicknesses of reflectors in contact with, or surrounding, process equipment or fissionable material units. One should be aware that controlling other parameters may increase reflection. For example, when controlling neutron interaction between units by adding material between them, the undesired and unintended effect could occur by which a single unit is made critical because of reflection. See also 5.7.5.2.5, "Moderation control," for related effects.

The effectiveness of standard and credible composite reflectors incidental to normal or abnormal conditions of processing, storing, or transporting fissionable material should be considered and evaluated, as appropriate. Examples could include combinations of water and steel, lead and depleted uranium, or concrete and SiO_2.

5.7.5.2.7 Mass control. Mass control may be used on its own or in combination with other nuclear parameter controls. In either case, administrative means of control are required.

Mass control often takes on aspects of nuclear materials accountability, particularly when used in laboratory situations. Mass control limits are frequently established for individual laboratory rooms, or groups of rooms, and detailed records are kept of mass transfers into and out of the room. Extensive administrative controls are generally implemented involving the transfer of fissionable material, documentation of fissionable masses currently in the facility, posting of limits, and

surveillance of the laboratories, records, and posted limits. Mass limits for adjoining rooms shall also account for potential interaction. Alternatively, room walls could be designed to preclude potential interaction.

Mass control may be used to limit the quantity of fissionable material in processes such as casting of metal, disposal, storage, collection, or withdrawal, or in transportation containers. Sampling or nondestructive measurements are often required to verify masses. Establishment of mass limits for containers of fissionable material should involve consideration of potential moderation and reflection, geometry, enrichment, spacing, concentration, and neutron poisons. Safe mass varies considerably, depending on the other nuclear parameters involved. Controls shall be implemented to ensure that unexpected changes in these other nuclear parameters will not cause a criticality accident.

5.7.5.2.8 Enrichment or isotopic composition control. When a facility handles fissionable material with a range of enrichments or isotopic compositions, it is useful to consider the potential benefit of employing enrichment or isotopic composition control in conjunction with other nuclear parameters. For example, safe mass for a given enrichment or isotopic composition, favorable geometry for a given enrichment or isotopic composition, and favorable spacing for a given enrichment or isotopic composition may all be useful concepts. In all cases, active-engineered or administrative controls, or both, are necessary to verify enrichment or isotopic composition and prevent the inadvertent use of fissionable material having a higher, more reactive enrichment or isotopic composition than specified for a particular operation.

In cases where enrichment or isotopic composition cannot be easily controlled, the available fissionable material providing the maximum reactivity shall be assumed.

5.7.5.2.9 Density control. Density control of solids is similar to concentration control for liquids, and areal density control may be applied to either solids or liquids. High density of solid fissionable material tends to reduce the volume or geometric dimensions (and sometimes the mass) that may be safely handled compared to lower densities of the same or similar material whether alone or in a mixture. Higher density of fissionable nuclides means that it is less likely for a neutron to escape without causing fission. Moderation and mass control are normally required as well when using density control for solids. Also, maximum density of the fissile nuclide as a solid or in a mixture of solids is normally an assumption in many evaluations, hence not a control. The difference is that assumptions are those factors thought to be immutable and not readily subject to measurement or control. When density is used as a control, it is often represented indirectly, that is, in terms of what can be directly observed and controlled. For example, storage containers in a moderation control area may have a lower mass limit for the fissile nuclide as metal than for the same nuclide in a compound. However, some processes such as super-compacting solid wastes are becoming more prevalent to minimize storage or repository space, and the effects of greatly increasing density of the fissionable material within a container should not be overlooked, especially if many such containers are to be stored in an array with minimum spacing between them. It may be necessary to establish control on the overall fissionable nuclide density of the array as well as on the fissionable nuclide density within units.

Areal density control, a related concept to overall array density, is defined by making a projection perpendicular to a planar surface, such as a floor or tank bottom, and limiting the mass of fissionable nuclides per unit area on this projection. Areal density control may be very beneficial when the area of the planar surface is large. In such cases, the mass of fissionable nuclides in an area or within a vessel may be safely increased by a large factor over the minimum critical mass, and it does not

matter whether the fissionable material is in the solid or liquid form. Areal density control may also be applied to discrete items, equipment, or containers of either solids or liquids, and if so, is akin to spacing control. In all cases, care must be taken to ensure that no localized region containing more than a minimum critical mass can credibly exceed the overall limit of mass per unit area.

5.7.6 Identifying Potential Criticality Scenarios. Objective 2 - criticality scenarios are identified. The first step in evaluating an element of risk is the recognition of it. Based on past experience, it can be expected that while many control failures resulting in contingent conditions leading to a criticality accident will be obvious, other contingent conditions will not be apparent.

5.7.6.1 Four measures contributing to successful identification. For highly complex systems the objective of identifying all potential criticality scenarios is idealized, and in practice will likely not be met. However, four measures can be taken to reduce the chance that potential criticality risks will go unrecognized, as follows:

(a) appropriate commitment of time and resources commensurate with the size of the project and complexity of the processes/systems;

(b) use of design and review personnel that have operating and nuclear criticality safety experience with similar processes/systems working with a cognizant nuclear criticality safety specialist;

(c) use of a systematic approach in the identification process to minimize the chance that potential criticality scenarios will go unrecognized (Several approaches to criticality scenario identification are briefly discussed in section 5.7.6.2, and an example is provided.); and

(d) selection of preferred criticality safety control methods to provide protection against a broad range of initiating events, some of which may go unrecognized (this fourth measure has been discussed in detail in section 5.7.5, "Means of Controlling the Criticality Risks").

It is important to note that the identification process should cover a full range of planned and unplanned conditions in a facility, including normal and abnormal operations, start-up, maintenance, shutdown, and decommissioning.

5.7.6.2 Approaches for criticality scenario identification. Scenario identification and analysis involve the identification and analysis of sequences of events that can lead to a criticality accident. Two basic approaches may be used, separately or together, to perform a scenario analysis for criticality safety. These approaches are (1) using systematic logic models to identify and analyze accident sequences, and (2) postulating the accident sequences directly using previous operating experience, incident data, and engineering judgment. The first approach works well when addressing complex designs that have interacting systems and when addressing new and untried designs. The second approach is satisfactory for simple systems and systems built similar to existing systems.

5.7.6.2.1 Using logic models to identify accident scenarios. Several different logic models have been developed and applied to perform scenario analysis of nonreactor nuclear facilities. These models are useful for identifying accident scenarios in general, and are often useful in identifying criticality scenarios that may otherwise go undetected. Some representative methods are outlined in the following paragraphs.

5.7.6.2.1.1 Deductive Logic Tree Analysis. Deductive logic tree analysis (fault tree analysis using *a priori* reasoning as exemplified in PRAs) is a deductive logic technique that diagrammatically models the various combinations of basic failure events that contribute to some overall failure event. A deductive logic tree begins with the definition of this ultimate failure event or consequence, such as a critical excursion in a specific piece of equipment, and is expanded downward through subsequent levels of contributing failures until an appropriate level of basic failure events has been reached. The contributing failures may be combined as necessary by logical AND and OR gates at the appropriate levels, if necessary. Deductive logic trees are normally used to model events having binary operational states (total failure vs. total success), as opposed to those having partial failures. The deductive nature of the tree is an advantage in that no assumption of accident initiating events is necessary. However, a detailed understanding of the system being examined is necessary so that important system failure modes are not missed. Even so, this technique can be successfully employed throughout the various design and review stages.

As mentioned above, deductive logic trees can be used to model accident sequences, where the top event becomes some consequence of failure sequences. This may result in combining several system logic trees that contribute to the overall consequence thereby providing several independent paths that can lead to the final consequence of a critical excursion. An example of a deductive logic tree applied to a facility being analyzed for nuclear criticality safety is provided in section 5.7.6.2.3. Detailed discussion of fault tree analysis can be found in NUREG-0492 (section 2.3.2.6 of this standard).

5.7.6.2.1.2 Inductive Logic Tree Analysis. Inductive logic tree analysis (event tree analysis using *a posteriori* reasoning) is an inductive logic technique that sequentially models the progression of events, both successes and failures, leading from some initiator to a series of logical outcomes. An inductive logic tree begins with some initiating failure, usually on a component or misoperation level, and maps out a sequence of events to form a set of branches, each of which represents a specific accident sequence leading to a particular final consequence such as a nuclear criticality accident. Like deductive logic trees, inductive logic trees are normally used to model events having total success or failure.

Each accident sequence identified by the inductive logic tree is somewhat analogous to a branch of a deductive logic tree. However, while a deductive logic tree branch represents a combination of failures leading to the undesired consequence, an inductive logic tree branch represents a combination of sequential events (both failures and successes) leading to the undesired consequence. While complete inductive logic tree analysis requires identification of all possible and distinct initiating events and development of an inductive logic tree for each, inductive logic trees are often useful in examining the consequences of failure of a particular piece of equipment. A detailed understanding of the overall system may be necessary in order to understand how the failure of a particular component affects the success or failure of other components.

5.7.6.2.1.3 Failure Modes and Effects Analysis. A failure modes and effects analysis (FMEA), used with PRAs, is an inductive analysis that systematically analyzes component failure modes and identifies the resulting effects on the system. An FMEA can be relatively detailed, if needed, and quantitative if data exist. Emphasis is placed upon identifying the problems that result from hardware failure. Typically, a columnar format is employed in an FMEA. Specific entries include

(a) component identification,
(b) failure rate,

(c) failure mode,
(d) effect on the system,
(e) severity class, and
(f) compensating provisions.

A FMEA provides a systematic examination of failures of a system and is relatively simple to apply, but it has the disadvantage of considering only one failure at a time rather than multiple failures.

5.7.6.2.2 Postulating accident scenarios directly. A set of accidents may be postulated based on the designer/analyst knowledge of previous operating experience, incident data, previously conducted safety assessments, and engineering judgment. This technique often involves the generation of a series of "what if" questions. These postulated accidents may also be quantified if accident frequency data are available. In many cases, accident frequencies are estimated using engineering judgment. This approach offers the advantage of simplicity, but its success is highly dependent on the experience of the designer/analyst. The results of such analyses are difficult to reproduce and defend.

The maximum credible accident approach and the design basis accident approach are two related techniques that may be useful in identifying scenarios and in distinguishing between those that are credible and those that are incredible. The maximum credible accident approach uses engineering judgment to identify accidents. Based on an intuitive estimate of their probabilities, the accident scenarios are divided into credible and incredible accident scenarios. The incredible accidents are not analyzed in detail. Accidents having a probability of occurrence greater than the maximum credible accident can then be analyzed in detail. This approach is typically used only to estimate the upper bound of the accident consequence potential of the particular operation and to design specific protective systems only for the maximum credible accident. As noted previously, however, it is important to identify as many accident scenarios as possible that potentially could lead to a criticality accident. Analysts should not subjectively dismiss potential criticality scenarios as incredible when it may be possible through a design change to eliminate the scenario completely. The advantage of the maximum credible accident approach is its simplicity, while its weakness is the subjective nature of the division between credible and incredible accident scenarios and the typical treatment of only the maximum credible accident.

The design-basis accident approach is an extension of the maximum credible accident approach. A series of accidents, including low-probability accidents with major consequences, are postulated based on various accident initiators and used as the explicit basis for design or analysis. Accidents having a lower probability of occurrence than the design-basis accident in each accident initiator area are generally not analyzed. The design-basis accident approach is more comprehensive than the maximum credible accident approach but the weakness remains -- the subjective nature of the selection of accidents.

As applied to nuclear criticality safety, the terms "maximum credible accident" and "design-basis accident" are not particularly useful except as a means to aid in distinguishing between credible and incredible accidents. Any potential criticality event, regardless of the magnitude of the initial fission burst, should be carefully analyzed and appropriate design changes made if necessary.

5.7.6.2.3 Deductive logic tree example. An illustration of a simplified version of a deductive logic tree analysis applied to the design of a facility is shown in Figure 5.7.6.2.3-1. The first step is to logically divide the process into discrete locations, starting by dividing the process area into general

locations or systems such as rooms, cabinets, glove boxes, process lines, or other appropriate groupings within the facility, and proceeding to the specific locations where criticality (the undesired consequence) could occur. This facility breakdown process is nothing more than a systematic way to ensure that all locations are considered with respect to nuclear criticality safety.

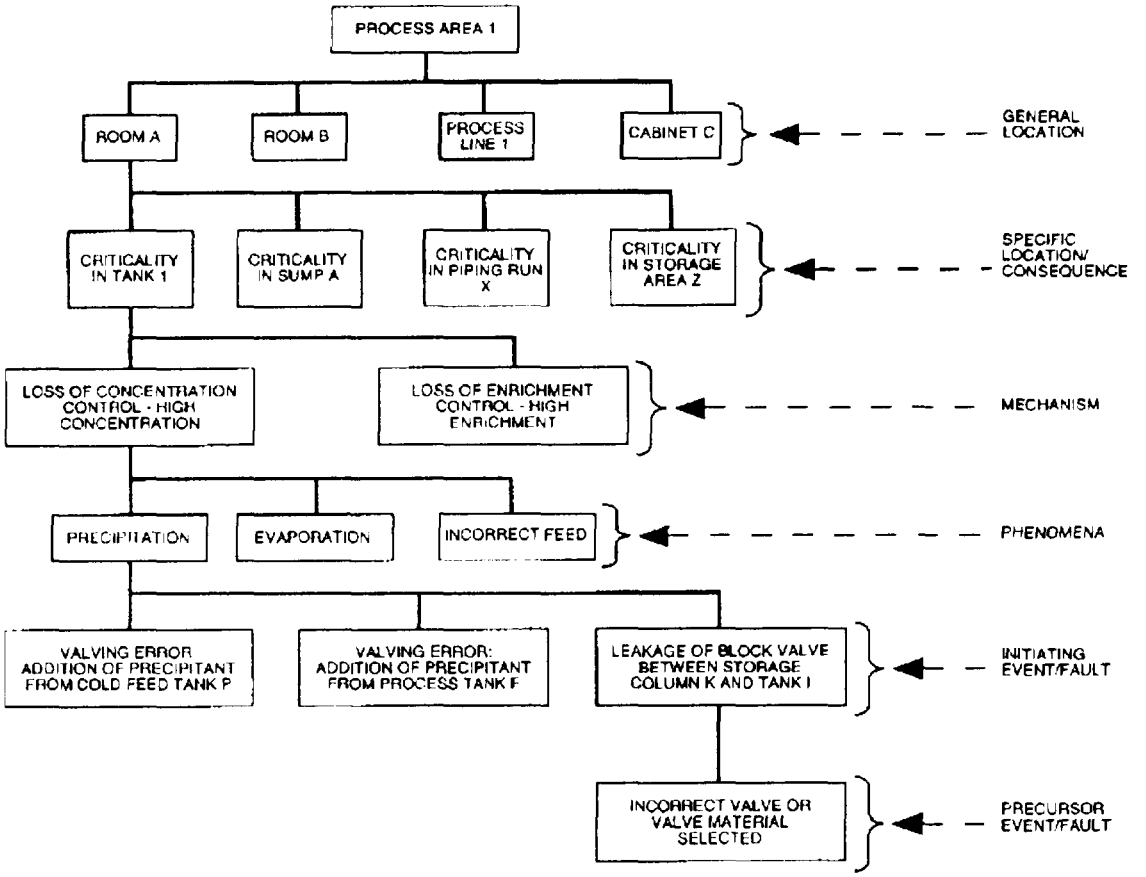

Figure 5.7.6.2.3-1. Illustration of deductive logic tree.

The specific locations to be included should encompass all locations having sufficient volume to support a criticality event such as in-process vessels, storage tanks, feed tanks, sumps, process piping, ventilation piping and duct work, pumps, filters, and waste drums, or the potential for loss of spacing that could lead to a criticality event for circumstances such as wet or dry reactor fuel storage, waste drum storage, and oxide or nitrate storage.

The second step involves chaining backward to develop the bottom three rows of Figure 5.7.6.2.3-1 which complete the deductive logic tree and illustrate a means to assist in logically thinking through all of the possible paths potentially leading to a criticality event in a specific location. These rows are labeled mechanisms, phenomena, and initiating events, and are defined as follows:

Mechanisms - As used here, the word mechanism refers to the direct means by which criticality is possible in a specific location. Mechanisms include loss of mass control, loss of concentration control, loss of geometry control, loss of moderation and reflection control, loss of spacing control (interaction), loss of enrichment control, loss of fixed or soluble neutron poison control, and the potential for unplanned transport of fissionable material into an unfavorable geometry such as by siphoning or leakage. See Table 5.7.6.2.3-1. A potential for criticality exists whenever the safe limit is exceeded for a nuclear parameter chosen for criticality safety control. In Figure 5.7.6.2.3-1, nuclear criticality safety in Tank 1 is maintained by controlling the fissionable material concentration. Thus, the mechanism for criticality in Tank 1 is identified as "high fissionable material concentration." The purposeful listing of mechanisms is most useful for analyzing potential causes of a criticality.

Phenomena - Refers to the possible alternative means for attaining the mechanism for a potential criticality. For example, in Figure 5.7.6.2.3-1 three possible phenomena are identified for attaining high fissionable nuclide concentration: a precipitation phenomenon, an incorrect feed phenomenon, and an evaporation phenomenon. For information, Table 5.7.6.2.3-1 contains some of the more common phenomena associated with mechanisms. The purposeful listing of phenomena is useful for analyzing potential causes of a criticality.

Initiating Events - Initiating events refer to the basic failures that can cause the phenomena identified. The credibility or incredibility of such things as natural events and effects as potential criticality accident initiating events may depend on initial design criteria such as earthquake-resistant criteria, tornado-resistant criteria, siting above the flood plain, and elimination of vehicles from a certain area. If appropriate design criteria are in place, the probability of natural events or effects initiating events causing a phenomenon leading to a criticality accident is likely to be incredible. The facility SAR should document the design criteria used and the resultant probability of associated initiating events. For example, in Figure 5.7.6.2.3-1, the phenomenon of precipitation may be caused by either of two failures: valving error leading to the transfer of precipitant from cold feed Tank P to Tank 1; or a valving error leading to the transfer of precipitant from process Tank F to Tank 1. Sometimes the initiating event (failure) may have potential precursor failures, requiring that the tree be extended. Examples of various types of failures are included in Table 5.7.6.2.3-2.

When developing a deductive logic tree, several points should be kept in mind. There is no fixed format or nomenclature. Rather, the emphasis here is on the use of the systematic and deductive thinking process involved in deductive logic tree development. The aim is to identify all of the locations where criticality is a possibility and all of the conceivable ways that an unsafe condition could occur. The focus of the deductive logic tree should be on identifying potential criticality scenarios for later examination. As developed herein, deductive logic trees may be entirely qualitative. It is not necessary (nor even desired) that the criticality preventive measures be represented. The selection and adequacy of controls can be considered separately for each criticality scenario (see sections 5.7.5 and 5.7.8). As a final note, attempts at making distinctions between the initiating event as an equipment failure or as a breakdown of administrative controls can sometimes become a source of confusion and may be pointless or artificial.

For further illustration of this process for identifying potential criticality scenarios, the example in Appendix D may be helpful.

Table 5.7.6.2.3-1. Examples of Mechanisms Leading to a Criticality

Mechanism	Applicability
1. Loss of mass control; fissionable material limits exceeded	When it is important to limit the mass of a fissionable material to less than a specific value.
2. Loss of concentration control; fissionable material concentration limits exceeded	When it is important to limit the concentration of a fissionable material to less than a specific value.
3. Loss of geometry control; geometry limits exceeded	When it is important to limit the geometry (dimension) of pieces of fissionable material or equipment containing fissionable material.
4. Loss of volume control; fissionable material volume limits exceeded.	When it is important to limit the volume of fissionable material.
5. Loss of moderation control; moderation limits exceeded.	When it is important to limit the extent of moderation or reflection of fissionable material.
6. Loss of reflection control; reflection limits exceeded.	When it is important to limit the extent of fissionable material neutron reflection.
7. Loss of spacing control (interaction); spacing limits exceeded.	When it is important to limit the spacing of arrays of fissionable material or various pieces of equipment containing fissionable material.
8. Loss of fixed or soluble neutron poison control; absorber concentration/absorber dimension/absorber leaching limits exceeded.	When it is important to limit the potential for criticality by the use of neutron poisons.
9. Loss of enrichment control; enrichment limits exceeded	When it is important to limit the enrichment (assay) of the fissile isotope.
10. Unplanned transport of fissionable material to unfavorable geometry.	A general class of nuclear criticality safety concerns (including such things as unexpected siphoning, leakage, evaporation and recondensation, or scale formation) in which quantities of process solutions could inadvertently move from a safe situation (safe geometry) to an unsafe situation (unsafe geometry).

Table 5.7.6.2.3-2. Examples of Phenomena and Initiating Events Leading to the Mechanism for a Potential Criticality Event

Mechanism	Examples of Phenomena: and Initiating Events
1. Loss of mass control; fissionable material mass limits exceeded.	a. Double (multiple) batching: human error or failure of automatic solution addition equipment. b. Fissionable material content higher than expected: incorrect sample result, incorrect feed, sample mixup, or enrichment higher than expected. c. Slow accumulation: unrecognized slow leak.
2. Loss of concentration control; fissile material concentration limits exceeded.	a. Precipitation: precipitant added inadvertently as a result of valving errors. b. Evaporation: tank abandoned (natural evaporation), loss of coolant, exothermic reaction. c. Solvent extraction: gradual accumulation of solvent, solvent added inadvertently, degraded solvent accumulates in equipment.
3. Loss of geometry control; geometry limits exceeded.	a. High internal pressure causing geometry distortions: eructation, gas generation, exothermic reactions. b. Corrosion (thinning) of vessel walls causing increase in internal vessel dimensions: loss of chemistry control. c. Slumping: inadequate choice of material for high temperature environment.
4. Loss of moderation or reflection control, or both; moderation or reflection limits, or both, exceeded.	a. Flooding of location or equipment designated to remain dry: backflow, leak, or spill of process liquids; sprinkler activation when equipment exposed for maintenance activities. b. Moisture pickup from surrounding atmosphere: loss of control of cabinet atmosphere. c. Excessive reflection from nearby maintenance or operating personnel or the introduction of new material adjacent to the item of concern: procedural violations, maintenance activities, or design changes. d. Loss of reflection used for neutronic isolation: maintenance operations or facility design changes.
5. Loss of spacing control (interaction); spacing limits exceeded.	a. Additional units added to an array: procedural violations or design change without investigating present limits. b. New equipment containing fissionable material introduced into an area already having fissionable material: design change without investigating present limits.

6. Loss of fixed or soluble neutron poison control; absorber concentration, absorber dimension, or absorber leaching limits exceeded.	a. Leaching of absorber material: loss of chemistry control or inadvertent addition of leaching materials. b. Corrosion (thinning) of absorber plates, rods, or Raschig rings: loss of chemistry control, failure to make periodic inspections, poor inspection measurements. c. Physical loss: fire or mechanical impact. d. Improper chemical makeup: human errors in calculations or procedures; incorrect sampling results. e. Precipitation of absorber materials from solution: valving error or other inadvertent addition of precipitant. f. Formation of scale containing absorber material: inadequate temperature or chemistry control, or poor material selection. g. Dilution of soluble absorber materials: valving errors introducing water or other diluents, or leaking across a heat exchanger.
7. Loss of enrichment control; enrichment limits exceeded.	a. Inadvertent addition of high enriched material: valving error, procedural error, or leakage.
8. Unplanned transport of fissionable material into an unfavorable geometry.	a. Leakage: from a vessel or a line, through a closed valve, across the tubes of a heat exchanger, or between lines in very close proximity due to vibration. b. Improper transport of process liquids: valving errors. c. Backflow: pressure upset - multiple initiating events. d. Back siphonage: pressure upset - multiple causes. e. Liquid entrainment in an off-gas line: upset in operating conditions. f. Air lift phenomena: upset in operating conditions. g. Overflowing a vessel with the solution flowing through common venting or piping to other units: loss of level control.

5.7.7 Eliminating Potential Criticality Scenarios. Objective 3 - criticality scenarios are eliminated to the extent practical. Rather than accepting an element of risk, it is preferred, in principle, that the risk be removed entirely (if feasible). Although a potential criticality scenario associated with a design concept may be shown to meet the minimum standard for acceptability (section 5.7.8), an effort should be made to explore the feasibility of design changes that would act to eliminate the scenario altogether. On occasion, elimination can be achieved by design changes that remove the initiating event to the accident sequence.

It is not possible to identify all such possibilities; however, three examples are provided in section D.2 to illustrate the intent and lines of inquiry. These examples involve (1) eliminating a source of water from the design concept that could potentially reach a location that must remain "dry" for nuclear criticality safety, (2) eliminating a potential motive force (high pressure) that could cause the backflow of liquid containing fissionable material to an unsafe location, and (3) eliminating a potential for over-concentration of solution containing fissionable material.

5.7.8 Judging Acceptability of a Potential Criticality Scenario. Objective 4 - criticality risks are acceptably unlikely. The key concepts and terminology presented in this section are the Double-Contingency Principle, double-contingency analysis, and barriers for contingencies.

Protecting against a credible criticality accident involves a defense-in-depth approach in which multiple, unlikely events must occur before a criticality accident is possible. This section provides a minimum acceptance standard for a potential criticality scenario based on a defense-in-depth approach called the Double-Contingency Principle.

It is important that the Double-Contingency Principle be considered, implemented, and documented at each step of the analysis process (see section 5.7.4). This does not mean that the complete implementation of the Double-Contingency Principle must occur during the earliest design stage of a new process or process modification. Rather, it means that there should be a consistent, documented application of double-contingency as the design evolves to finalization and as operating procedures are prepared. The final result, that may include several reports/letters/reviews, should be a clear, documented trail of how double-contingency has been achieved in a given facility.

5.7.8.1 Double-contingency analysis meaning and application. A double-contingency analysis is an analysis of potential criticality accident scenarios for the purpose of demonstrating compliance with the Double-Contingency Principle by identifying appropriate barriers and means of control. A double-contingency analysis should be performed by the cognizant nuclear criticality safety specialist in concert with the design organization and facility/process operators, as needed. It should be an ongoing process, beginning as early as possible in the design activity and continuing through the preparation of operating procedures prior to start-up. The complete documentation of the double-contingency analysis may be composed of various design documents, reports, design reviews, safety analyses, letters, or other documents, but should be traceable. The CSO shall review the double-contingency analysis for sufficiency.

The Double-Contingency Principle's defense-in-depth approach calls for the presence of (at least) two controlled barriers (a loss of a barrier is referred to as a contingency) against the potential for a criticality accident. Each barrier shall be capable of terminating a potential criticality accident scenario. The basic notion is that in the event one of the barriers should fail when needed, the second barrier will be available to prevent the accident. ***For this approach to be effective, each of the two barriers shall be unlikely to fail, and shall be independent in terms of their failure modes.*** While failure mode independence can be established, likelihood of failure cannot be well quantified under conditions of sparse data, such *in situ* conditions being desirable from a safety standpoint. This has led Paxton to observe, in LA-3366 (section 2.3.2.5 of this standard), that Double-Contingency, as a formal rule, cannot substitute for expert judgment. Paxton further states that experience and common sense usually provide the only basis for "likely" or "unlikely" determinations.

The objective of the independency of the barriers has important effects on the selection of the control method(s) and means of control. It is generally regarded that the highest degree of

independency can be achieved through the control of two independent nuclear parameters such that loss of control of EITHER nuclear parameter alone will not cause a criticality accident. This is sometimes referred to as a two-parameter barrier. For example, assume that a large, geometrically unsafe tank has been designed to store solution whose fissile concentration is normally well below the minimum critical concentration, but that could become higher than the minimum critical concentration due to various potential system failures. To achieve double-contingency, it is decided to base one barrier on concentration control and the second barrier on soluble absorber control. For concentration control, the barrier may be to terminate flow in a feed stream whenever a high concentration of fissionable material is detected. For soluble absorber control, the barrier may be to add soluble absorber solution if the absorber concentration is less than a specified value. A criticality accident cannot occur if concentration control alone is lost because of the presence of soluble absorber. Similarly, a criticality accident cannot occur if soluble absorber control alone is lost because of the normally low fissile concentration of the process solution. As discussed in section 5.7.5, these two barriers may be implemented using engineered or administrative means of control. To ensure double-contingency, it is also preferred that the means of control for implementing the two barriers be independent of each other. Continuing the present example, to terminate the flow of a concentrated feed stream, the active-engineered means of control might include a sensor to detect high fissile concentration, the associated electrical interlock, and an automatic valve in the feed stream line to close upon demand. To add soluble absorber solution if the absorber concentration is low, the administrative means of control may be to sample the tank solution for boron content on a periodic basis (such as once per shift) and to manually add boric acid solution until the desired concentration is achieved. Thus, the means of control for implementing each barrier are independent of each other. This approach ensures protection against a wide array of accidents. It may also be possible to encounter a situation in which two independent barriers can be provided that have potential common-cause control failures. In this case, one or more separate means of control, in addition to that which has potential common-cause failure, should be used to ensure the action of each barrier.

Occasions do exist, however, in which a two-parameter barrier is not feasible, and reliance is placed on a single nuclear parameter, that is the loss of control of a single nuclear parameter can lead to a criticality accident. This is often the case, for example, when using concentration control. In this case, multiple (at least two controls) are needed on this nuclear parameter. Here, the objective would be to apply the preferred control means (such as engineered controls over administrative controls) and to select specific controls that are as independent as possible in terms of common-cause failure modes. Section 5.7.11 provides an example in which criticality safety is dependent solely on moderation control (that is, the prevention of water introduction to a "dry area"). Here, each of the two barriers is an active-engineered device, and they appear to be absent of common-cause failure modes.

5.7.8.2 Basic steps in implementing double-contingency and performing a contingency analysis. The approaches used to identify potential criticality accident scenarios are discussed in section 5.7.6. The basic steps for implementing double-contingency and performing a double-contingency analysis of a potential criticality scenario are the following:

a. identify the two (or more) barriers for application of the Double-Contingency Principle,

b. show that each barrier is independent and unlikely to fail as described in section 5.7.8.3,

c. identify all means of control associated with each barrier as described in section 5.7.8.4, and

d. perform a final review of the potential criticality scenario relative to all six basic nuclear criticality safety design objectives (section 5.7.4), particularly the following two objectives:

Objective 3 - to eliminate as many as possible of the identified potential criticality scenarios through the use of careful design, use of alternative materials, and alternative equipment; and

Objective 1 - to minimize the probability of occurrence of potential criticality scenarios by using a preferred hierarchy of criticality safety controls.

5.7.8.3 Qualifications for a contingency barrier. In accordance with the statement of the Double-Contingency Principle, it is important that each of the two barriers meet two basic requirements: (1) be unlikely to fail when called upon, and (2) function in an independent manner. The determination of whether a barrier is unlikely to fail may be made on the basis of engineering judgment or quantitative failure rate information, if available. Either approach should be capable of being defended.

5.7.8.3.1 Quantitative guidelines for acceptable contingency barrier failure probabilities. The following quantitative guidelines may be used, subject to data availability, to judge whether the failure of a barrier is sufficiently unlikely such that it may qualify for application to the Double-Contingency Principle.

Guideline 1: The estimated probability that the barrier will fail (when called upon for protection) is no greater than 1 in 100 demands, or stated otherwise, the unavailability is less than 0.01/demand), and

Guideline 2: The product of the estimated frequency of the initiating event (expressed in occurrences per year) times the estimated failure probability (applied in Guideline 1) is no greater than 1 in 10 years.

Thus, the calculated maximum frequency for potential criticality is 1 in 1000 years, that is, the frequency of the initiating event times the failure probability of the first barrier times the failure probability of the second barrier. It is not expected that detailed quantitative risk analyses will be available at the time initial design selections are made for criticality safety control. However, a reasonable expectation of the performance of a proposed means of control may be available from the results of past risk analyses or experiences with similar means of control in similar applications. Such information is useful to screen out means of control that may later prove to be unsatisfactory. Table 5.7.8.3.1-1 provides guidance as to when a quantitative analysis of double-contingency control failures should be performed.

Table 5.7.8.3.1-1. Guidelines for Performing Quantitative Risk Analysis of Double-Contingency Control Failures

Type of Control[A]	Necessity of Quantitative Analysis of Control Failures
Two independent control methods, each having independent passive-engineered means of control	Optional
One control method having two or more independent passive-engineered means of control	Optional
One control method having two or more redundant passive-engineered means of control	Should be considered
Two independent control methods, each having independent active-engineered means of control	Should be considered
One control method having two or more independent active-engineered means of control	Should be considered
One control method having two or more redundant active-engineered means of control	Usually required
Two independent control methods, each having independent administrative means of control	Usually required
One control method having two or more independent administrative means of control	Usually required
One control method having two or more redundant administrative means of control	Usually required

[A]For combinations of passive- and active-engineered means of control, quantitative analysis of control failures should be considered.

For combinations of passive-engineered and administrative means of control, quantitative analysis of control failures should be considered.

For combinations of active-engineered and administrative means of control, quantitative analysis of control failures is usually required.

Formal quantitative risk analysis can be a valuable tool when properly used. The development and analysis of logic trees can effectively identify flaws in control schemes. The logic analysis process can also assist in identifying alternative criticality control methods that may be more cost effective. However, caution should be applied in the use of these methods. Although quantitative, the estimates made using these methods still rely on engineering judgment. The criticality professional should be aware of the potential error bands in the basic failure rate data and estimates and their effect on the final quantities.

5.7.8.3.2 Guidelines for independency. The basic notion is that dual protection could be lost if a single (common-cause) failure exists that could act to compromise both barriers. Obviously, a process would be unacceptable where a single component, or subsystem, is shared by both barriers and whose failure would simultaneously defeat both barriers. Even with two completely redundant systems with complete component and physical separation, it is possible that an error in calibration (performed identically on both protective systems during maintenance) could compromise both systems. Whenever possible, diversity is preferred to redundancy. Diverse controls involving the measurement of two, or more, different nuclear parameters and causing two, or more, types of safety action are less subject to common-cause failures.5.7.8.3.3 *Quantification of the* simultaneous collapse frequency of two controls. The effectiveness and estimated frequency for the simultaneous collapse of two controls used for Double-Contingency Principle applications can be assessed for certain circumstances. That is, controls used for nuclear criticality safety that are periodically monitored for their continued effectiveness or failure and are repaired or brought into specification for continued use as part of the Double-Contingency Principle can be evaluated statistically to determine the expected simultaneous failure frequency of both controls. An example of such an approach is provided in Appendix C.

5.7.8.4 Conspicuous and prominent identification of double-contingency means of control. Each means of control associated with the operating process that contributes to a barrier for double-contingency shall be conspicuously and prominently identified in operating procedures. Consideration should also be given to conspicuously and prominently identifying the means of control associated with double-contingency that appear in design drawings and design reports. These means of control may be in a variety of forms, including various engineered and administrative controls. The intent of conspicuously identifying the means of control associated with double-contingency is that it serves to highlight to operating personnel those features, controls, and administrative actions that are of importance to nuclear criticality safety and that require special care and preservation.

5.7.8.5 Exemptions to applying the Double-Contingency Principle. Application of the Double-Contingency Principle -- that is, the necessity for a second, independent barrier -- is not required if the potential criticality scenario in the absence of a second barrier is incredible. For this purpose, incredible is defined as an estimated frequency of occurrence of less than once in one million years per event, provided reasonable allowance is made for uncertainties. The facility Safety Analysis Report could provide guidance for distinguishing between credible and incredible scenarios. However, if there is no real basis for estimating if an accident scenario is incredible, whether by engineering judgment or data, then double-contingency should be provided except where shielding and confinement satisfy the requirements of section 2.3.1.7.

5.7.9 Operability of Criticality Safety Controls. Objective 5 - criticality safety controls are operable. Selections made during the design and safety analysis process will play an important role in the ability of facility personnel to successfully operate the facility and deal with the associated criticality

safety controls. Several important considerations affecting operability of the criticality safety controls are discussed in this section.

5.7.9.1 Identifying controls important to nuclear criticality safety. Successful operation of the nuclear criticality safety controls for a facility cannot be achieved without a clear understanding of the control features that are of importance to nuclear criticality safety. This information shall be documented as clearly as possible and transmitted from the design and analysis process to the facility operators. As discussed in section 5.7.10, "Documenting the Criticality Risks," the important elements of documentation include (1) identification of the barriers for double-contingency, derived from the double-contingency analysis, (2) identification of the associated means of control, and (3) information pertinent to the preservation and maintenance of each means of control, such as its required functional capabilities, design specifications, configuration control, and the testing and surveillance requirements.

5.7.9.2 Examining the operability of the set of controls. Each means of control associated with double-contingency for the design concept will require facility operational support to maintain a necessary high level of reliability. As discussed in section 5.7.5.2, some control methods require considerably more operational support than others. A review should be made from the perspective of the total program required in the facility to support the set of controls required for nuclear criticality safety. The objective is to ensure that the total program required is reasonably achievable and manageable.

5.7.9.3 Incorporating good human factors practices. The use of good human factors practices in the design and operations will greatly contribute to successful operation of the criticality safety controls by reducing the potential for human error in operating and maintenance activities. Examples of useful references are found in sections 2.2.2.8 and 2.2.2.9. Considerations include, for example, the layout and labeling of controls, valves, and displays (such as the identification of lines, use of colors, and labels to demarcate panel systems and functions) and the strategic placement of operational assistance (such as succinct instructions for use of equipment, storage arrays, packaging, and handling). Another important area deals with physical space and arrangement, based on importance and frequency of use. It is essential that these considerations begin early in the design and analysis process. Experience has shown that retrofitting a system to improve human factors following construction can be impractical or, at a minimum, very costly.

5.7.9.4 Incorporating uniformity into the design. Incorporating uniformity (consistency) into the design will reduce complexity, training time, and the chances for human error. An integrated approach should be taken to the (total) facility design to ensure uniformity relative to nuclear criticality safety. For example, the selection of a criticality safety control method for each of two different areas in a facility that have similar processes and criticality considerations should be consistent, unless there is a compelling reason to do otherwise. However, this is not intended to exclude diversity to prevent common-mode failures.

5.7.9.5 Facilitating sampling. For selected process and storage vessels, the ability to sample the solution in the vessel (such as for fissionable material concentration, presence of solids, organics, and other materials) will be important to nuclear criticality safety. In these cases, consideration should be provided in the design concept to ensure that operating personnel can obtain samples that are representative of the vessel contents. Ensuring sampling capability may involve proper location of sampling points and the incorporation of mixing and recirculation features. The timely results of sample analyses assist in smooth and safe operations.

5.7.9.6 Facilitating inspection and maintenance. For selected process areas and equipment, the ability of operating personnel to perform periodic inspections and maintenance activities will be important to nuclear criticality safety. This may include, for example, the need for periodic inspections of equipment, piping, duct-work, and the annular space between double-walled tanks for possible accumulations of solid fissionable material; inspections of liquid levels in tanks; inspections of equipment dimensions; inspections for leaks; inspections of fixed absorbers; and inspections for maintenance of engineered criticality safety controls. Both visual inspections and the use of portable monitoring devices may be necessary. During the design process it is important to identify those portions of the facility requiring such inspections and to provide appropriate design features to facilitate inspection activities such as viewing-ports, absence of hidden areas, and physical accessibility.

The possibility of fissionable material buildup in exhaust or other duct-work systems requires particular attention. Where it is determined to be necessary for nuclear criticality safety, the design of exhaust duct-work should provide for (1) access points for visual inspection using video cameras, fiber-optic devices, or the unaided eye, and for equipment used for removal of fissionable material (such equipment should be geometrically safe); (2) adequate work space to accommodate periodic monitoring of the duct-work using portable equipment such as gamma-monitoring equipment, and, if gamma monitoring is intended, sufficient distance from nearby gamma sources to minimize or lessen background radiation; (3) consideration of making the duct-work itself geometrically safe, where it is not possible or practical to prevent the potential accumulation of fissionable material; (4) the capability to clean the duct-work without tearing it down (this can often be done by avoiding sharp angles and (5) the use of internal pull brushes to move material to access points); and the minimization of sudden expansions, sharp bends, dampers, long horizontal runs, and internal obstructions that contribute to making particles fall out of the air or inert gas stream.

5.7.9.7 Facilitating flushing. In some cases, the ability to flush a line or a tank will be important to nuclear criticality safety. Necessary provisions should be included in the design concept to permit a high-quality flushing operation, such as compatibility of flushing chemicals with the materials of construction, proper line sizes and slopes, adequate line supports to limit sagging, incorporation of special valves needed for the flushing operation, proper location of the flush addition and exit points, and isolation of the chemical flush feed tanks to prevent backflow of fissionable material into the tanks.

5.7.9.8 Anticipating process changes. When designing facilities and equipment intended to process low concentrations, low enrichments, or low masses of fissionable material, such that nuclear criticality safety is not a problem, it is important to anticipate that process changes may be requested in the future, that is, a new feed stream may be added or a higher enrichment may require processing. In such cases, it is prudent to incorporate some form of criticality safety control into the design or to make suitable provision for adding criticality safety controls in the future.

5.7.9.9 Accommodating fire control systems. One of the important nuclear parameters related to nuclear criticality safety is neutron moderation. In the absence of moderating materials such as water, relatively large masses of fissile nuclides in the form of powders or metals may be safely handled. If the presence of water is possible, however, some operations with dry fissile nuclides may have to be severely constrained, modified, or eliminated.

A potential conflict exists between nuclear criticality safety and fire safety over the use of moderating agents such as water for fire suppression systems. An analysis is necessary to

determine if a credible inadvertent criticality accident could be caused by an automatic sprinkler system or the use of fire hoses. This analysis should involve nuclear criticality safety, fire safety, and safety analysis personnel. If a credible inadvertent criticality accident is not possible, then a water sprinkler system and fire hoses should be used. However, if a credible inadvertent criticality accident is possible, then alternative fire suppression systems should be employed. There are also situations in which a water sprinkler system is acceptable, but the use of high-pressure fire hoses is unacceptable because of the potential to rearrange items in an array.

In some situations, it is reasonably simple to make changes to equipment and operations such that the use of water is permissible. For example, revising the unit spacing of a storage array and taking steps to ensure that fissile units cannot be rearranged can make the use of water acceptable in the form of automatic sprinklers or fire hoses. In other cases, taking provisions to prohibit the accumulation of water in equipment by the use of appropriately placed and sized drainage holes, the use of an enclosure, or increasing the slope of piping may make the use of water acceptable.

In certain situations in which nuclear criticality safety is a concern, it may be possible to use borated water as a fire suppression agent. If borated water is to be used, a dedicated source of borated water shall be available, and the concentration of boron shall be periodically confirmed.

If the use of water is not permissible in operations with fissile nuclides, then the operating and design personnel shall work with nuclear criticality safety and fire safety specialists to find a suitable alternative. From a nuclear criticality safety perspective, there are usually no restrictions on the use of dry chemicals, carbon dioxide, most foams, or inert gases as fire suppression agents in facilities that handle fissile nuclides. However, fire safety specialists will have to agree on the adequacy of these other fire suppression agents for a given facility and operation. Industrial safety specialists will also be concerned with the use of some of these alternative fire suppression agents because they will displace air and could potentially asphyxiate workers. Signs should be conspicuously displayed to alert fire fighters and workers if the use of water is not permitted and to identify what fire suppression agents are acceptable.

5.7.10 Documenting the Nuclear Criticality Safety Analysis and Controls. Objective 6 - criticality analysis and controls are documented. Documentation of the nuclear criticality safety analysis for fissionable material in process, storage, or transportation is essential for use by engineering design personnel, persons engaged in the design review process, facility operating personnel, cognizant nuclear criticality safety staff, and process reviewers and auditors. The five basic analysis objectives discussed previously in this guide serve as a focal point for the documentation effort. Guidelines for documentation are presented in Table 5.7.10-1, and specific guidance on the content of the nuclear criticality safety analysis is provided in sections 5.7.10.1 through 5.7.10.2.

The following provides an acceptable method for documenting those elements of a nuclear criticality safety analysis (NCSA) described in the previous sections of this chapter and in Table 5.7.10-1. The level of detail for the process should be commensurate with the complexity of the fissionable material operation. Documentation of the analysis should consist of the following three parts:

1. NCSA Proposal - The description of the proposed fissionable material facilities; equipment; processes; potential criticality scenarios; process-, operational-, and equipment-controls related to

Table 5.7.10-1. Summary of Nuclear Criticality Safety Analysis Documentation Objectives

Category	Documentation Objective	Section of Design: Guidelines	Section of Design: Objective
Documentation relative to each specific location where criticality is credible.	Risks are identified: Present all potential criticality scenarios that were identified using devices such as logic diagrams, tabulations.	Section 5.7.6	Obj. 2
Documentation relative to each potential scenario identified above.	Risks are minimized: Show that the most preferred criticality safety control method(s) has (have) been employed and that it is (they are) practical for the set of conditions.	Section 5.7.5	Obj. 1
	Risks are eliminated: Describe considerations given to feasible design alternatives to eliminate the potential scenario.	Section 5.7.7	Obj. 3
	Risks and controls are acceptable: Show compliance with the Double-Contingency Principle, including: Identification of the two barriers and the basis for qualification. Identification of the means of control, including functional requirements such as specifications, time responses, set points, and information pertinent to care, maintenance, and testing.	Section 5.7.8	Obj. 4
Information relative to the facility as a whole.	Operability of controls: Describe the general approach taken to the nine design considerations listed in section 5.7.9 aimed at facilitating successful operations of the set of criticality safety controls by facility operating personnel.	Section 5.7.9	Obj. 5

the potential criticality scenarios; and contingent conditions (provided by engineering process/equipment design and operations supervision and assisted by the cognizant NCS specialist, as needed).

2. Nuclear Criticality Safety Evaluation (NCSE) - The descriptions and results of the nuclear criticality safety evaluations (calculations, comparative analyses, standard references, and other resources) for all normal and contingent conditions identified in the proposal or subsequently considered and reviewed by the design and operations personnel. The content of NCSEs is discussed in section 5.9.

3. NCSA - The consolidation and referencing of the proposed fissionable material operations and the nuclear criticality safety evaluation to ensure that the objectives of Table 5.7.10-1 are addressed.

5.7.10.1 Documentation of NCSA proposal. Fissionable material operations management and appropriate process/equipment engineering design personnel shall provide the necessary written information so that the cognizant NCS specialist organization can adequately evaluate the subcriticality and analyze the safety of proposed fissionable material operations. This information should include the following, as appropriate:

a. Sufficient information provided for an adequate understanding of the process by the NCS analysts. This information may include as-built (Title III) engineering drawings, flow diagrams, facility layout drawings, sketches, and operating procedures.

b. Description of normal and all credible abnormal changes (contingencies, potential criticality scenarios) in process conditions that could alter a nuclear parameter.

c. Identification of passive and active safety controls that are part of the process. Safety systems and safety class items shall be identified along with the applicable nuclear parameters. Safety limits, limiting safety system settings, and limiting conditions of operations shall be specified as appropriate.

d. Identification and description of process including: flows; intermediate storage; transport; and usage, identification, and spacing of portable containers.

e. Identification of materials (fissionable and nonfissionable) potentially affecting the process, along with their physical and chemical forms and properties. The accuracy and precision of measurements used to characterize materials shall also be provided.

Information provided for the NCSA should be "signed-off" by two individuals knowledgeable of, and responsible for, the development of the proposed fissionable material operation and by two individuals knowledgeable of, and responsible for, the fissionable material operation after completion of the safety analysis.

5.7.10.2 Documentation of the NCSA. The NCSA should be provided by the NCS organization (with assistance, as needed, from the process/equipment engineering design and operating personnel) as a controlled document that includes

a. the NCSA Proposal in its entirety;

b. the NCSE in its entirety;

c. a discussion providing the basis for not using preferred criticality safety control method(s);

d. a description of considerations given to feasible design alternatives that could eliminate potential criticality scenarios;

e. a demonstration of compliance with the Double-Contingency Principle, including the identification of multiple barriers and their bases for qualification, and the identification of the means of control, including functional requirements and information pertinent to care, maintenance, and testing such as specifications, time responses, set points, and inspection and maintenance intervals;

f. the reiteration of the NCSA Proposal limits and controls and any additional NCS limits and controls developed during the iterative evaluation and analysis process;

g. a discussion about the operability of criticality safety controls by facility operating personnel; and

h. the signing of the NCSA Proposal by

- the cognizant NCS specialist and peer reviewer to indicate completeness of the nuclear criticality safety analysis (If the evaluation or peer review is accomplished through the use of personnel outside of the installation NCS organization, the installation and NCS organization management should provide the qualifications and bases for any alternative use of non-installation NCS specialists.), and

- the fissionable material operations supervision and equipment/process engineering design personnel, indicating the understanding and acceptance of the NCSA results.

5.7.11 **Examples.** APPENDIX D provides some examples of a double-contingency analysis, the elimination of unnecessary scenarios, and passive and active controls.